CHAPTER 22

BY:

ETISHA JAIN

VISHU GOYAL

Linux 22.1 Understanding the need for SELinux

. Linux security is built on Unix security
. Unix security consists of different solutions that were never developed with current IT security needs in mind
. Most of the solutions focus on a part of the operating system
. SELinux provides a complete and mandatory security solution
. The principle is that if it isn't specifically allowed , it will be denied
. As a result , "unknown " services will always need additional configuration to enable them in an environment where SELinux is enabled

LINUX 22.2 Managing SELinux Modes

- Selinux can be enabled or disabled is all at the kernel level
- so if you want to switch enable to disable is only one option that is reboot
- enabled mode is enforcing
- when selinux is enabled then it will be block everything and provide more security whatever doesn't match a rule in the SElinux policy.
- if the mode is permissive it will still do a logging but it won't block anything
- Permissive is very usefull mode it you need to figure out what is happening becox in permissive mode your traffic is going to be allowed. but you can analysis your log file what is going wrong
- Permissive mode should be temporary mode only
- Enforcing mode is what your system. by default should be in.
- In order to switch between the enforcing and permissive you don't reboot your system
- you just use that setenforce permissive
- you just use that setenforce enforcing

- getenforce will show the current state.
- setenforce toggles between enforcing and permissive
- Edit /etc/sysconfig/selinux to manage the default state of SELinux
- Never set to disabled if this is meant as a temporary measure only!

PRACTICAL

- **getenforce**
- **setenforce permissive**
- **getenforce**
- **setenforce disabled not possible**
- **if you want to disabled the selinux then**
- **vim /etc/sysconfig/selinux**
- **LINUX=disabled please don't do it on the exam becoz it loose the security**
- **reboot**

- **getenforce**
- **setenforce enforcing**
- **SELinux is disabled**
- **if you want to start the selinux service then**
- **vim /etc/sysconfig/selinux**
- **LINUX=enforcing**
- **reboot**

And now look at this, because we have been in disabled mode, SELinux is aware of it.
and we can see that relabel is required.
you will always get a relabel if you have been in disabled mode
Because in disabled mode, SELinux is no longer capable of tracking the state of your files. so files may have gotten changed.
And in a relabel, SELinux is going to apply the entire SELinux policy labels to your file system again

LINUX 22.3 Understanding SELinux Context Labels and Booleans

- So to work with SELinux you need to know about the basic building block
- These basic building blocks are labels and booleans

- Let's talk about the context labels first.
- ***The first building block is***
- Every object is labeled with a context label
- **There are three parts i.e.**
- **user**: user specific context
- **role:** role specific context
- **type**:flags which type of operation is allowed on this object
- Many commands support a **-Z** option to show current context information
- Context types are used in the rules in the policy to define which source object has access to which target object

- ***The second buiding block is***
- _A boolean is an on/off switch
- Use it to enable or disable specific catefories of functionality altogether

PRACTICAL

First building block

- ps aux
- ps auxZ it show the process information with SELinux inforcing
- ps auxZ | grep ssh

- ls -lZd /etc/ssh/
- ls -lZ /etc/ssh/

- ps Zaux | grep httpd
- ls -Z /var/www
- httpd_sys_script_exec_t to run the script
- httpd_sys_content_t to read the content of the page

- ls -lZ /home/user/

Second building block which is the boolean

- getsebool -a
- getsebool -a | grep httpd
- setsebool -P httpd enable homedirs on

LINUX 22.4 Using File Context Labels

- use **semanage fcontex**t to set the file context label
- This will write the context to the SELinux Policy
- To enforce the policy setting on the file system, use restorecon
- Alternatively, use touch /.autorelabel to relabel all files to the context that is specified in the policy.

PRACTICAL

- **mkdir /web**
- **cd /web/**
- **vim index.html**
- welcome to the web directory web server
- **vim /etc/httpd/conf/httpd.conf**
- now you can change the document root path and also change the path in the directory path
- **systemctl restart httpd**
- **systemctl status httpd**
- **curl http://localhost**
- ohh now it is showing the defualt web page which was the apache web page
- to ingnore that warning by the SELinux or misconfiguratin
- **setenforce 0**
- **getenforce**
- **!cu**

- **setenforce 1**
- **man semanage-fcontext**
- see the example
- to set the corrent context label
- semanage fcontext -a -t httpd sys_content_t "/web(/.*)?" help us to write the new policy
- **!cur**
- **ls -ldZ /web**
- **restorecon -R -v /web**
- **ps Zaux | grep httpd**
- **ls -Zd .**

LINUX 22.5 Analyzing SELinux Log Messages

- SELinux uses auditd to write log messages to the audit log
- Messages in the audit log may be hard to interpret
- Ensure that sealert is available, it interprets messagges from the audit log, applies SELinux AI, and write meaningful messages to /var/log/messages
- Run the sealert command, including the UUID message to get advice on how to troubleshoot specific issues.

Practical

- So in our previous demo, we had this issue with Aveci
- grep AVC /var/log/audit/audit.log
- Now we should get selinux related messges
- AVC stands for access vector cache that happens to be how selinux messages are logged to the audit log
- avc: denied getattr is for get attribute
- pid
- path
- scontext source context
- tcontext target context
- **journalctl | grep sealert** to look in the systemd jounal what has been logged.
- we have seen lot of messages and these all are apache blocked messages
- sealert -l 16f10216-540-461-424- | less
- ausearch -c 'httpd' --raw | audit2allow -M my-httpd
- semodule -X 300 -i mu-httpd.pp

LINUX 22.6 Resetting the Root Password and SELinux

- reboot
- rhgb quiet remove that
- rb.break
- ctrl x
- mount
- mout -o remount,rw /sysroot
- chroot /sysroot
- passwd
- ls -Z /etc/shadow
- the content show is ? becox selinux is not loaded yet
- load_policy -i
- ls -Z /etc/shadow
- it is set as unlabled_t that is bad
- restorecon -v /etc/shadow
- touch /.autorelabel

Thank You